

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-069962

(43)Date of publication of application : 11.03.1994

(51)Int.Cl.

H04L 12/66

H04L 9/00

H04L 9/10

H04L 9/12

H04L 12/28

H04L 12/56

(21)Application number : 04-240046

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing :

17.08.1992

(72)Inventor : OTA HIROMI

(54) NETWORK CONNECTOR AND NETWORK COMMUNICATION SYSTEM

(57)Abstract:

PURPOSE: To conceal between which terminators communication is implemented and to conceal the content of the communication by sending data subjected to capsule processing while composing the data into a packet.

CONSTITUTION: A ciphering decision section 42 checks whether or not a path selected by a path selection section 11 is equivalent to a path stored in a secrecy protection required path storage section 43 and decides ciphering of packet data when the path is equivalent to the secrecy protection required path. The ciphering is implemented by a ciphering/decoding processing section 40. Then a data capsule processing section 41 implements processing of incorporating ciphered data into a packet as transmission data by selecting a network connector located in a region at the outside of secrecy protection range as if it were a final destination and using its own network connector as if it were a first sender. In this case when it is clear that the data are ciphered data the ciphering/decoding processing section 40 decodes the data into the original packet and the decoded data are sent to a final equipment being

a true final destination.

<hr size=2 width="100%" align=center>

CLAIMS

[Claim(s)]

[Claim 1] It is provided in a part which connects two or more subnetworks since a network which communicates by a connectionless type packet is constituted. In a network connection apparatus which analyzes information on a received packet, selects a sending-out course and sends out a new packet. A security required path storage section which makes a range which cannot carry out security memorize for every sending-out course. An encryption deciding part which opts for a data encryption about a network layer of a packet when it is what passes a security required course in which transfer paths selected based on a final destination of a packet are remembered to be encryption and a decoding processing part by said security required path storage section. A network connection apparatus which is provided with an encapsulation part which processes a network connection apparatus located in a place which escaped from a range which cannot carry out security as a final destination of said enciphered data and is characterized by building encapsulated data into a packet and sending it out.

[Claim 2] In a network communication system in a network which two or more subnetworks which communicate using a connectionless type packet are connected via a network connection apparatus and changes. When a range which cannot carry out security is included in a course to a final destination of a received packet in a network connection apparatus of the transmitting side, encipher data about a network layer of a received packet and build a network connection apparatus in a part beyond said range into a packet new as a final destination of said enciphered data and it is sent out. A network communication system decrypting enciphered data in a network connection apparatus made into a final destination and sending out to the next.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the network connection apparatus and network communication system in the network which comprises two or more subnetworks which communicate using a connectionless type packet.

[0002]

[Description of the Prior Art] Packet communication includes connection-oriented type (or connection oriented type) packet communication and connectionless type

packet communication. Connection-oriented type packet communication performs transmission (phase 3) of information or a message main part after performing connection (phase 1) of a communication line and setting out and establishment (phase 2) of a data link. Connectionless type packet communication performs the phase 3 suddenly. This invention is related to the latter.

[0003] There are some which two or more subnetworks were connected via the network connection apparatus and were constituted in the network of data communications. However if it communicated in the form as it is there are some which cannot keep secrecy in a subnetwork.

[0004] Secrecy cannot be kept in a subnetwork connectable by the 3rd unspecified persons such as ordinary public circuit exchange network and a public telephone network. Such a subnetwork is called Black subnetwork. On the other hand the subnetwork in which connection by the 3rd unspecified person is impossible is called White subnetwork like the line switching network in a company or LAN in a company (Local Area Network).

[0005] Drawing 6 is a figure showing one example of the network with which the subnetwork of Black and the subnetwork of White are contained. In drawing 6a terminating set E-Hand K of 50-56 are subnetworks a network connection apparatus and 57-59. It is an end user of data communications and a packet is first sent from these and the terminating sets 57-59 are eventually sent into these. The network connection apparatus 50-56 make connection between subnetworks. In this example the subnetwork H is Black and the subnetwork K is White.

[0006] When sending a packet to the terminating set 59 from the terminating set 57 the following two courses can be considered. The 1st course is a course of the terminating-set 57 → network connection apparatus 52 → subnetwork K → network connection apparatus 56 → terminating set 59. The 2nd course is a course of the terminating-set 57 → network connection apparatus 51 → subnetwork H → network connection apparatus 55 → terminating set 59. Since it passes along the subnetwork H of Black when sent in the 2nd course security is not guaranteed.

[0007] Then the applicant has already proposed the network communication system sent after checking a partner by exchanging passwords a priori as a communication method for security (Japanese Patent Application No. No. 26900 [four to]). Drawing 2 is a figure showing the network connection apparatus used with such a communication method. in drawing 2 -- 10 -- a destination deciding part and 11 -- a channel selection part and 12 -- a path storage section and 14 are [a reliability determination part and R of an interface and 16] network connection apparatus a certification information reply part and 17 a packet treating part and 15 the course Management Department and 13.

[0008] each interface 15 -- LAN a public network and a dedicated line -- it is an interface for connecting.

The internal configuration changes with partners who connect.

It is provided suitably to what kind of subnetwork these interfaces are connected.

[0009]The packet received via a certain interface is sent out via another interface after being processed by the packet treating part 14. The packet treating part 14 reads the information on the received packet and processes it in the form which can be sent out to the next destination (for example the following address is given). When the destination deciding part 10 – the path storage section 13 carry out the processing they play an auxiliary role.

[0010]The path storage section 13 has memorized the database about a network course and when there are deletion of a course, change and addition etc. the course Management Department 12 updates a database and manages it. The channel selection part 11 refers to the data of the path storage section 13 and chooses the course which sends a packet. The destination deciding part 10 determines the part which should be transmitted to the next.

[0011]The reliability determination part 17 determines whether the selected course can trust it on security. The password first provided in the partner's network connection apparatus which it is trying to send beforehand is sent. It is judged as the partner who can trust it if certification information is replied from a partner and data is sent. The certification information reply part 16 is a portion which replies certification information when self receives a password.

[0012]As document about the conventional technology of such data communication they are JP64-68044A and the publication number 3 for example. – There is a No. 13146 gazette.

[0013]

[Problem(s) to be Solved by the Invention](Problem) However in the communication directly performed by Hazama of network connection apparatus who has defined the password of security beforehand in the network connection apparatus and network communication system of the above mentioned former which perform security by password exchange can carry out security but. Among the middles were other network connection apparatus and in the communication indirectly performed via it there was a problem that security could not be carried out.

[0014](Explanation of a problem) In drawing 6 the network connection apparatus 51 and the network connection apparatus 55 presuppose that it is a network connection apparatus like drawing 2 constituted so that password exchange for security could be performed. When both up a circuit a course judges Black or White.

[0015]However when a course consists of two or more subnetworks and other network connection apparatus intervene in between security may not be able to be carried out in password exchange. Next the example is shown.

[0016]Drawing 10 is other examples of the network which comprises two or more subnetworks. As for A-D a terminating set and 7-9 are network connection apparatus a subnetwork and 1-6. The subnetwork A and D is LAN (Local Area Network) for example and the subnetwork B is a public network (X.25).

[0017]The terminating set which is an end user is connected to each subnetwork. For example the terminating sets 1 and 2 are connected to the subnetwork A. Connection between a subnetwork and a subnetwork is made by a network connection apparatus. For example connection between the subnetwork A and the subnetwork B is made by the network connection apparatus 7.

[0018]To the terminating set and network connection apparatus in a network the network address accepted in the whole network and the subnetwork address accepted within the subnetwork which is involving are given. Since the number of the subnetworks in which a terminating set participates is one the number of the subnetwork addresses is one but since the subnetwork in which a network connection apparatus participates is plurality two or more subnetwork addresses are given.

[0019]A packet is first sent out from a certain terminating set and attains the purpose by being sent to other terminating sets. When sending to the terminating set of other subnetworks it is sent via a network connection apparatus. For example when sending to the terminating set 6 from the terminating set 1 of drawing 10 as a dotted line shows it is sent in the course of the terminating-set 1 → network connection apparatus 7 → network connection apparatus 8 → network connection apparatus 9 → terminating set 6.

[0020]Since the subnetwork B is a public network when it passes along this secrecy may leak and there is doubt of Black. Temporarily even if the network connection apparatus 7 and 8 can perform communication which carried out security by password exchange secrecy may leak in the network which intervenes on the way and they cannot necessarily perform secret protection thoroughly.

[0021]Because in the subnetwork which the packet transmitted passes on the way the information about a data content a final destination etc. may be stolen by a certain means.

[0022]In the network containing LAN which was described above. As the protocol system The basic reference model of open systems interconnection as shown in drawing 8 (Open Systems Interconnection Basic ISO 7498 Information processing systems) reference model is adopted. This comprises seven layers the 1st layer physical layer the 2nd layer data link layer the 3rd layer network layer the 4th layer transport layer the 5th layer session layer the 6th layer presentation layer and the 7th layer application layer. Therefore composition of a packet is also made into the form where this protocol system was followed.

[0023]Drawing 7 is a figure showing the composition of a packet. 20 a packet and 21 an address subnetwork address and 22 A transmitting subnetwork address As for 23 and 25 a data division and 24D other information bureaus and 24 Packet data As for a final destination device network address and 28 26 is [other information bureaus and 30] data of the 4-7th layer a transmission source device network address and 29 a protocol header and Fixed Part and 27. The packet data 24D are stored in the data division 24.

[0024]The packet at the time of shipping towards the terminating set 6 from the terminating set 1 of the network of drawing 10 is taken for an example and the value indicated to each address of address subnetwork address 21 grade is explained. A subnetwork address will attach and express the numerals (ABCD) of a related subnetwork and a network address will attach and express N. In the transmitting subnetwork address 22 the address of the part which sends out this packet i.e. the subnetwork address of the terminating set 1 (1A) is indicated.

[0025]In the address subnetwork address 21 if the terminating set 6 is in the same subnetwork A as the terminating set 1 the subnetwork address of the terminating set 6 will be indicated. However since the terminating set 6 is in Haruka or the left subnetwork D in order to go there it must go exceeding other subnetworks. In such a case the subnetwork address (7A) about the subnetwork A of the network connection apparatus 7 which is the present address is indicated. Thus the address subnetwork address 21 and the transmitting subnetwork address 22 are rewritten whenever it exceeds a subnetwork.

[0026]The network address (6N) of the terminating set 6 to send into the final destination device network address 27 eventually is indicated and the network address (1N) of the transmitting agency terminating set 1 sent out first is indicated at the transmission source device network address 28. After each packet reaches the terminating set 6 which is a final destination it is assembled by the order specified at the time of sending out.

[0027]Drawing 9 is a figure showing change of the composition of the packet which has a network of drawing 10 conveyed. Numerals support the thing of drawing 7. From the terminating set 1 drawing 9 (b) is the packet composition in the case of sending to the network connection apparatus 7 and was already described.

[0028]Drawing 9 (**) is the packet composition in the case of sending to the network connection apparatus 8 from the network connection apparatus 7. The transmitting subnetwork address 22 is rewritten with the subnetwork address (7B) about the subnetwork B of the network connection apparatus 7. The address subnetwork address 21 is rewritten by the subnetwork address (8B) about the subnetwork B of the network connection apparatus 8. The transmission source device network address 28 and the final destination device network address 27 remain the same.

[0029]Drawing 9 (**) is the packet composition in the case of sending to the network connection apparatus 9 from the network connection apparatus 8. The transmitting subnetwork address 22 is rewritten with the subnetwork address (8C) about the subnetwork C of the network connection apparatus 8. The address subnetwork address 21 is rewritten by the subnetwork address (9C) about the subnetwork C of the network connection apparatus 9. The transmission source device network address 28 and the final destination device network address 27 remain the same.

[0030]Drawing 9 (**) is the packet composition in the case of sending to the terminating set 6 from the network connection apparatus 9. The transmitting

subnetwork address 22 is rewritten with the subnetwork address (9D) about the subnetwork D of the network connection apparatus 9 and the address subnetwork address 21 is rewritten by the subnetwork address (6D) of the terminating set 6. The transmission source device network address 28 and the final destination device network address 27 remain the same.

[0031] Thus a packet is an intermediate subnetwork and network connection apparatus and since it is analyzed the communication to which terminating set from which terminating set it is in going via a subnetwork and a network connection apparatus without the guarantee of security there is a possibility that data may be stolen. This invention makes it SUBJECT to solve such a problem.

[0032]

[Means for Solving the Problem] It is provided in a part which connects two or more subnetworks since a network which communicates by a connectionless type packet in this invention in order to solve said SUBJECT is constituted. In a network connection apparatus which analyzes information on a received packet selects a sending-out course and sends out a new packet. A security required path storage section which makes a range which cannot carry out security memorize for every sending-out course. An encryption deciding part which opts for a data encryption about a network layer of a packet when it is what passes a security required course in which transfer paths selected based on a final destination of a packet are remembered to be encryption and a decoding processing part by said security required path storage section. We had an encapsulation part which processes a network connection apparatus located in a place which escaped from a range which cannot carry out security as a final destination of said enciphered data and decided to build encapsulated data into a packet and to send it out.

[0033] In a network communication system in a network which two or more subnetworks which communicate using a connectionless type packet are connected via a network connection apparatus and changes. When a range which cannot carry out security is included in a course to a final destination of a received packet in a network connection apparatus of the transmitting side. Encipher data about a network layer of a received packet and build a network connection apparatus in a part beyond said range into a packet new as a final destination of said enciphered data and it is sent out. In a network connection apparatus made into a final destination we decided to decrypt enciphered data and to send out to the next.

[0034]

[work —] for In a network which two or more subnetworks which communicate using a connectionless type packet are connected via a network connection apparatus in this invention and changes. When it is going to carry out secret communication between points which sandwiched a subnetwork which cannot carry out security a network connection apparatus which had special composition in those points is installed.

[0035] When a range which cannot carry out security is in a course which transmits

from there in this network connection apparatus Data including address information of the first transmitting terminating set and the last address terminating set is enciphered and it has packet composition addressed to a network connection apparatus located in a place which escaped from a range which cannot carry out security of it and sends (encapsulation). A network connection apparatus which received it decrypts enciphered data and sends it to a terminating set of a final destination with the usual packet composition.

[0036] If it is within limits which cannot carry out security since it passes in a form of the usual packet addressed to a network connection apparatus located in a place which escaped from the range the fact among which terminating sets communication was really performed can be hidden. Since it is enciphered data can hide the contents.

[0037]

[Example] Hereafter working example of this invention is described in detail based on Drawings. Drawing 1 is a network connection apparatus of this invention. Numerals correspond to the thing of drawing 2 and as for encryption and a decoding processing part and 41 an encryption deciding part and 43 are security required path storage sections a data encapsulation part and 42 40. These are the composition provided specially because of security. The network connection apparatus which has such composition is installed in the connection section of the subnetwork which can carry out security and the subnetwork which is not made. Hereafter each formation part is explained. Since the thing of the same numerals as drawing 2 achieves the same operation and a function the explanation is omitted.

[0038] The security required path storage section 43 memorizes whether security is guaranteed to which network connection apparatus when sending a packet in which course. For example the security required path storage section 43 of the network connection apparatus 7 of drawing 10 remembers the network connection apparatus 9 that security is not guaranteed when sending out in the direction of the subnetwork B.

[0039] The encryption deciding part 42 investigates whether the course selected in the channel selection part 11 is equivalent to the course memorized to the security required path storage section 43 and when it corresponds it determines to encipher the packet data 24D of drawing 7. Encryption is performed by encryption and the decoding processing part 40. Arbitrary things can be used for the technique of encryption. Encryption and the decoding processing part 40 also perform decrypting when the enciphered data is received.

[0040] The data encapsulation part 41 makes a final destination the network connection apparatus located in the place which escaped from the range which cannot carry out security and a self network connection apparatus as first transmitting origin Processing incorporated in a packet by using the aforementioned encryption data as send data (this is made [of explanation] "encapsulation" for convenience) is carried out.

[0041] Drawing 3 is a figure showing the composition of the packet which encapsulated

encryption data. Numerals correspond to the thing of drawing 7 and a capsule construct and 32 31 A protocol and FixedPartAs for a final destination network connection apparatus network address and 34 other information bureaus and 36 are encryption data storing parts a transmitting agency network connection apparatus network address and 35 33.

[0042]When it becomes clear that it must send out to the course which cannot do security as a result of analyzing the received packet with the network connection apparatus of this inventionThe packet data 24D about a network layer are encipheredand it is stored in the encryption data storing part 36 as the same treatment as the send data of the usual packet.

[0043]At and equivalent to the final destination device network address 27 (refer to drawing 7) in the usual packet compositionthen the final destination network connection apparatus network address 33 at the time. The network address of the network connection apparatus located in the place which escaped from the range which cannot carry out security is indicated. At equivalent to the transmission source device network address 28 (refer to drawing 7) in the usual packet compositionthen the transmitting agency network connection apparatus network address 34 at the time. The network address of the network connection apparatus which is going to shipself network addressi.e.packetis indicated.

[0044]Drawing 4 shows the example of the packet which stored encapsulation data. Since this is a network of drawing 10 and it is a range which cannot carry out security between the network connection apparatus 7 and 9In order to carry out communication from which secrecy does not leak among bothin the environment where the network connection apparatus of this invention is used as the network connection apparatus 7 and 9the packet sent to the terminating set 6 from the terminating set 1 is a thing in the state where it was remade with the network connection apparatus 7.

[0045]Numerals support the thing of drawing 3. The address of the transmission source device network address 28 is made into the network address (1N) of the terminating set 1It is enciphered in a form as it isand the packet data 24D in which the final destination device network address 27 was made into the network address (6N) of the terminating set 6 are stored in the encryption data storing part 36. Let the transmitting agency network connection apparatus network address 34 be a network address (7N) of the network connection apparatus 7 which is just going to ship this packet now. Let the final destination network connection apparatus network address 33 be a network address (9N) of the network connection apparatus 9 located in the place which escaped from the range which cannot carry out security.

[0046]The network connection apparatus 7 with which the transmitting subnetwork address 22 is just going to ship this packet nowIt is considered as the subnetwork address (7B) about the subnetwork Band let the address subnetwork address 21 be a subnetwork address (8B) about the subnetwork B of the network connection

apparatus 8 which is the present destination.

[0047] If a packet is sent with such composition in the intermediate network connection apparatus which cannot carry out security it will be dealt with as a usual packet whose first transmitting origin is the network connection apparatus 7 and whose final address is the network connection apparatus 9. Therefore the network connection apparatus located in the place which escaped from the range which cannot carry out security is sent not understood at all and where true transmitting origin and a true final destination are goes. Even if it tries to steal send data with an intermediate network connection apparatus since it is enciphered the portion cannot know the contents.

[0048] Although the network connection apparatus 9 located in the place which escaped from the range which cannot carry out security is also used as the network connection apparatus which has the composition of this invention if a packet is received it will be judged whether it is what has been enciphered and encapsulated. The judgment is made by investigating whether it has passed along the course registered into the security required path storage section 43 as where a transmitting agency is (in the case of an upper example network connection apparatus 7).

[0049] When it becomes clear that it is enciphered it decrypts to the original packet data 24D by encryption and the decoding processing part 40 and this is sent to the terminating set 6 which is a true final destination with the usual packet composition.

[0050] Drawing 5 is a flow chart showing a send action which the network connection apparatus of this invention mentioned above.

Step 1 -- A packet is received.

Step 2 -- The received packet is analyzed a course is chosen and the address which transmits to the next is determined.

Step 3 -- That the selected course takes the measure of security checks with reference to the security required path storage section 43 for whether it is a required course. If it does not pass it transmits to the next without taking the measure of security.

Step 4 -- When it passes along the course which needs security send data is enciphered including the information on the final destination and first transmitting origin.

Step 5 -- The enciphered data is encapsulated.

Step 6 -- It transmits to the following address.

[0051] In order to carry out the network communication system of this invention it is not necessary to change the network connection apparatus of the whole network into the thing of the composition of this invention and since what is necessary is to install the network connection apparatus of this invention only in the point which is going to carry out communication which only carried out security it can carry out easily at cheap cost.

[0052]

[Effect of the Invention]As stated aboveaccording to the network connection apparatus and network communication system of this invention. When the range which cannot carry out security is in the course which transmits from there when it is going to carry out secret communication between the points which sandwiched the subnetwork which cannot carry out securityData including the first transmitting terminating set and the last address terminating set is encipheredand it has packet composition addressed to a network connection apparatus located in the place which escaped from the range which cannot carry out security of itand sends (encapsulating).

[0053]Thereforeif it is within limits which cannot carry out securitysince it passes in the form of the usual packet addressed to a network connection apparatus located in the place which escaped from the rangethe fact among which terminating sets communication was really performed can be hidden. Since it is enciphereddata can hide the contents.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]A network connection apparatus of this invention

[Drawing 2]The conventional network connection apparatus

[Drawing 3]The figure showing the general composition of the packet which stored encapsulation data

[Drawing 4]The figure showing the example of the packet which stored encapsulation data

[Drawing 5]The flow chart showing the send action of the network connection apparatus of this invention

[Drawing 6]The figure showing one example of the network with which the subnetwork of Black and the subnetwork of White are contained

[Drawing 7]The figure showing the composition of a packet

[Drawing 8]The figure showing the basic reference model of open systems interconnection

[Drawing 9]The figure showing change of the composition of the packet which has a network of drawing 10 conveyed

[Drawing 10]The figure showing other examples of the network which comprises two or more subnetworks

[Description of Notations]

1-6 -- A terminating set7-9 -- A network connection apparatus10 -- Destination deciding part11 [-- Packet Management Department] -- A channel selection part12 -- The course Management Department13 -- A path storage section14 15 -- An interface16 -- A certification information reply part17 -- Reliability determination

part20 -- A packet24D24D₁24D₂ -- Packet data31 [-- An encryption deciding part43
/ -- A security required path storage section50-56 / -- A network connection
apparatus57-59 / -- A terminating setA-HK / -- A subnetwork and R are network
connection apparatus.] -- A capsule construct40 -- Encryption and a decoding
processing part41 -- A data encapsulation part42

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-69962

(43)公開日 平成6年(1994)3月11日

(51)Int.Cl.⁵

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 12/66

9/00

9/10

8529-5K

H 0 4 L 11/ 20

B

7117-5K

9/ 00

Z

審査請求 未請求 請求項の数 2(全 9 頁) 最終頁に続く

(21)出願番号 特願平4-240046

(22)出願日 平成4年(1992)8月17日

(71)出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂三丁目3番5号

(72)発明者 太田 裕美

神奈川県川崎市高津区坂戸3丁目2番1号

K S P R & D ビジネスパークビル 富

士ゼロックス株式会社

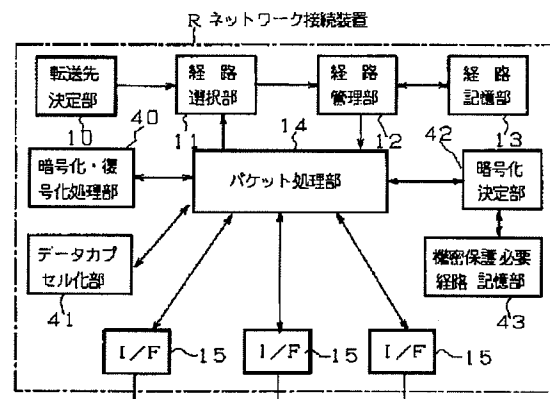
(74)代理人 弁理士 本庄 富雄 (外1名)

(54)【発明の名称】 ネットワーク接続装置およびネットワーク通信方式

(57)【要約】

【目的】 コネクションレス型パケットを用いて通信する複数のサブネットワークから成るネットワークにおけるネットワーク接続装置およびネットワーク通信方式において、機密保護を行うこと。

【構成】 機密保護し得ないサブネットワークを挟んだ地点間で機密の通信をしようとする場合に、それらの地点に、図のような特別な構成を持ったネットワーク接続装置Rを設置する。このネットワーク接続装置では、そこから送信する経路中に機密保護し得ない範囲がある場合には、最初の送信端末装置および最後の宛先端末装置を含めてデータを暗号化し、それを機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置宛のパケット構成にして送る。それを受け取ったネットワーク接続装置は、暗号化されたデータを復号化し、最終宛先の端末装置へ、通常のパケット構成で送る。



【特許請求の範囲】

【請求項1】 コネクションレス型パケットにより通信を行うネットワークを構成するため複数のサブネットワークを接続する個所に設けられ、受け取ったパケットの情報を解析して送出経路を選定し新たなパケットを送出するネットワーク接続装置において、機密保護し得ない範囲を送出経路毎に記憶させておく機密保護必要経路記憶部と、暗号化および復号化処理部と、パケットの最終宛先に基づいて選定した転送経路が前記機密保護必要経路記憶部に記憶されている機密保護必要経路を通過するものである場合にパケットのネットワーク層に関するデータの暗号化を決定する暗号化決定部と、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置を前記暗号化したデータの最終宛先として処理するカプセル化部とを具え、カプセル化したデータをパケットに組み込んで送出することを特徴とするネットワーク接続装置。

【請求項2】 コネクションレス型パケットを用いて通信する複数のサブネットワークがネットワーク接続装置を介して接続されて成るネットワークにおけるネットワーク通信方式において、送信側のネットワーク接続装置では、受け取ったパケットの最終宛先までの経路中に機密保護し得ない範囲が含まれている場合に、受け取ったパケットのネットワーク層に関するデータを暗号化し、前記範囲を越えた個所にあるネットワーク接続装置を前記暗号化したデータの最終宛先として新たなパケットに組み込んで送出し、最終宛先とされたネットワーク接続装置では、暗号化されたデータを復号化して次へ送出することを特徴とするネットワーク通信方式。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】 本発明は、コネクションレス型パケットを用いて通信する複数のサブネットワークから成るネットワークにおけるネットワーク接続装置およびネットワーク通信方式に関するものである。

【0002】

【従来の技術】 パケット通信には、コネクションオリエンテッド型（またはコネクション型）パケット通信と、コネクションレス型パケット通信とがある。コネクションオリエンテッド型パケット通信は、通信回線の接続（フェーズ1）、データリンクの設定と確立（フェーズ2）を行ってから、情報あるいはメッセージ本体の伝送（フェーズ3）を行うものである。コネクションレス型パケット通信は、いきなりフェーズ3を行うものである。本発明は、後者に関係している。

【0003】 データ通信のネットワークには、複数のサブネットワークがネットワーク接続装置を介して接続されて構成されたものがある。しかしながら、サブネットワークには、そのままの形で通信したのでは、機密の守れないものがある。

【0004】 一般公衆回線交換網や公衆電話網などの不特定の第3者によって接続可能なサブネットワークでは、機密を守ることができない。このようなサブネットワークは、Black なサブネットワークと言われる。一方、企業内回線交換網や企業内LAN（Local Area Network）のように、不特定の第3者による接続が不可能なサブネットワークは、White なサブネットワークと言われる。

【0005】 図6は、Black のサブネットワークとWhite のサブネットワークとが含まれているネットワークの1例を示す図である。図6において、50～56はネットワーク接続装置、57～59は終端装置、E～H、Kはサブネットワークである。終端装置57～59が、データ通信のエンドユーザーであり、最初にこれらからパケットは発信され、最終的にこれらに送り届けられる。ネットワーク接続装置50～56は、サブネットワーク間の接続を行う。この例では、サブネットワークHはBlack であり、サブネットワークKはWhite である。

【0006】 終端装置57から終端装置59へパケットを送る場合、次の2つの経路が考えられる。第1の経路は、終端装置57→ネットワーク接続装置52→サブネットワークK→ネットワーク接続装置56→終端装置59という経路である。第2の経路は、終端装置57→ネットワーク接続装置51→サブネットワークH→ネットワーク接続装置55→終端装置59という経路である。第2の経路で送られた場合、Black のサブネットワークHを通るので、機密保護は保証されない。

【0007】 そこで、機密保護のための通信方式として、事前にパスワードを交換することにより、相手を確認してから送るネットワーク通信方式を、出願人は既に提案している（特願平4-26900号）。図2は、そのような通信方式で用いられるネットワーク接続装置を示す図である。図2において、10は転送先決定部、11は経路選択部、12は経路管理部、13は経路記憶部、14はパケット処理部、15はインタフェース、16は認証情報返信部、17は信頼性決定部、Rはネットワーク接続装置である。

【0008】 各インタフェース15は、例えばLANとか公衆回線網とか専用線とかと接続するためのインタフェースであり、接続する相手によってその内部構成は異なる。これらのインタフェースは、どのようなサブネットワークに接続するかによって、適宜設けられる。

【0009】 或るインタフェースを介して受け取られたパケットは、パケット処理部14で処理された後、別のインタフェースを介して送り出される。パケット処理部14は、受け取ったパケットの情報を読み取り、次の転送先へ送り出せる形に処理する（例えば、次の宛先を付与する）。転送先決定部10～経路記憶部13は、その処理をする際に補助的な役割を果たす。

【0010】 経路記憶部13はネットワークの経路に関

するデータベースを記憶しており、経路管理部12は、経路の削除、変更、追加等があった場合にデータベースを更新して管理する。経路選択部11は、経路記憶部13のデータを参考にして、パケットを送る経路を選択する。転送先決定部10は、次に転送すべき箇所を決定する。

【0011】信頼性決定部17は、選択した経路が機密保護の上で信頼できるか否か決定する。送ろうとしている相手のネットワーク接続装置に、まず予め定めてあるパスワードを送ってみる。相手から認証情報が返信されて来ると信頼できる相手と判断し、データを送る。認証情報返信部16は、自己がパスワードを受け取った場合に、認証情報を返信する部分である。

【0012】このようなデータ通信の従来技術に関する文献としては、例えば特開昭64-68044号公報、特開平3-13146号公報がある。

【0013】

【発明が解決しようとする課題】（問題点）しかしながら、パスワード交換によって機密保護を行う前記した従来のネットワーク接続装置およびネットワーク通信方式では、予め機密保護のパスワードを定めているネットワーク接続装置同士の間で直接行う通信の場合には機密保護できるが、途中で他のネットワーク接続装置等があり、それを介して間接的に行う通信の場合には機密保護できないという問題点があった。

【0014】（問題点の説明）図6において、ネットワーク接続装置51とネットワーク接続装置55とが、機密保護のためのパスワード交換を行い得よう構成された、図2のようなネットワーク接続装置であるとする。両者は回線をupする際、経路がBlackかWhiteかを判断する。

【0015】しかし、経路が複数のサブネットワークからなり、間に他のネットワーク接続装置が介在するような場合は、パスワード交換では機密保護できない場合がある。次に、その例を示す。

【0016】図10は、複数のサブネットワークから成るネットワークの他の例である。A～Dはサブネットワーク、1～6は終端装置、7～9はネットワーク接続装置である。サブネットワークA、C、Dは、例えばLAN (Local Area Network) であり、サブネットワークBは、公衆回線網 (X.25) である。

【0017】各サブネットワークには、エンドユーザーである終端装置が接続されている。例えば、サブネットワークAには、終端装置1、2が接続されている。サブネットワークとサブネットワークとの接続は、ネットワーク接続装置によって行われる。例えば、サブネットワークAとサブネットワークBとの接続は、ネットワーク接続装置7によって行われる。

【0018】ネットワーク内にある終端装置やネットワーク接続装置に対しては、ネットワーク全体で通用する

ネットワークアドレスと、関与しているサブネットワーク内で通用するサブネットワークアドレスとが付与されている。終端装置が関与するサブネットワークは1つであるから、そのサブネットワークアドレスは1つであるが、ネットワーク接続装置が関与するサブネットワークは複数であるから、複数のサブネットワークアドレスが付与されている。

【0019】パケットは、最初に或る終端装置から送り出され、他の終端装置へ届けられることにより、目的を達する。他のサブネットワークの終端装置へ送る場合には、ネットワーク接続装置を経由して届けられる。例えば、図10の終端装置1から終端装置6へ送る場合には、点線で示すように、終端装置1→ネットワーク接続装置7→ネットワーク接続装置8→ネットワーク接続装置9→終端装置6という経路で届けられる。

【0020】サブネットワークBは公衆回線網であるため、ここを通るときに機密が漏れる可能性があり、Blackの疑いがある。仮に、ネットワーク接続装置7、8はパスワード交換により機密保護をした通信が出来るものであったとしても、途中に介在するネットワークで機密が漏れる場合もあり、完全に機密の保護ができるわけではない。

【0021】なぜなら、転送されるパケットは、途中で通過するサブネットワークにおいて、何らかの手段によってデータ内容や最終宛先等に関する情報が盗まれる可能性がある。

【0022】前記したようなLANを含むネットワークでは、そのプロトコル体系として、図8に示すような開放型システム間相互接続の基本参照モデル (ISO 7498 Information processing systems, Open Systems Interconnection Basic reference model) が採用されている。これは、第1層物理層、第2層データリンク層、第3層ネットワーク層、第4層トランスポート層、第5層セッション層、第6層プレゼンテーション層、第7層アプリケーション層の7層から構成されている。従って、パケットの構成も、このプロトコル体系に則った形にされる。

【0023】図7は、パケットの構成を示す図である。20はパケット、21は宛先サブネットワークアドレス、22は送信サブネットワークアドレス、23、25はその他の情報部、24はデータ部、24Dはパケットデータ、26はプロトコルヘッダおよびFixed Part、27は最終宛先装置ネットワークアドレス、28は送信元装置ネットワークアドレス、29はその他の情報部、30は第4～7層のデータである。データ部24には、パケットデータ24Dが格納される。

【0024】図10のネットワークの終端装置1から終端装置6に向けて発送する際のパケットを例にとり、宛先サブネットワークアドレス21等の各アドレスに記載する値について説明する。なお、サブネットワークアド

レスは、関係するサブネットワークの符号（A，B，C，D）を付して表し、ネットワークアドレスはNを付して表すことにする。送信サブネットワークアドレス22には、このパケットを送りだす箇所のアドレス、つまり終端装置1のサブネットワークアドレス（1A）を記載する。

【0025】宛先サブネットワークアドレス21には、もし、終端装置6が終端装置1と同じサブネットワークA内にあれば、終端装置6のサブネットワークアドレスが記載される。しかし、終端装置6は遙か離れたサブネットワークDにあるので、そこへ行くためには、他のサブネットワークを越えて行かなければならない。そういう場合には、当面の宛先であるネットワーク接続装置7の、サブネットワークAに関するサブネットワークアドレス（7A）が記載される。このように、宛先サブネットワークアドレス21と送信サブネットワークアドレス22とは、サブネットワークを越える毎に、書き換えられる。

【0026】最終宛先装置ネットワークアドレス27には、最終的に送り届けたい終端装置6のネットワークアドレス（6N）が記載され、送信元装置ネットワークアドレス28には、最初に送り出す送信元終端装置1のネットワークアドレス（1N）が記載される。各パケットは最終宛先である終端装置6に到着した後、送出時に指定した順序に組み立てられる。

【0027】図9は、図10のネットワークを搬送されるパケットの構成の変化を示す図である。符号は図7のものに対応している。図9（イ）は、終端装置1からネットワーク接続装置7へ送る場合のパケット構成であり、既に述べた。

【0028】図9（ロ）は、ネットワーク接続装置7からネットワーク接続装置8へ送る場合のパケット構成である。送信サブネットワークアドレス22が、ネットワーク接続装置7のサブネットワークBに関するサブネットワークアドレス（7B）と書き換えられ、宛先サブネットワークアドレス21が、ネットワーク接続装置8のサブネットワークBに関するサブネットワークアドレス（8B）に書き換えられている。送信元装置ネットワークアドレス28、最終宛先装置ネットワークアドレス27は、元のままである。

【0029】図9（ハ）は、ネットワーク接続装置8からネットワーク接続装置9へ送る場合のパケット構成である。送信サブネットワークアドレス22が、ネットワーク接続装置8のサブネットワークCに関するサブネットワークアドレス（8C）と書き換えられ、宛先サブネットワークアドレス21が、ネットワーク接続装置9のサブネットワークCに関するサブネットワークアドレス（9C）に書き換えられている。送信元装置ネットワークアドレス28、最終宛先装置ネットワークアドレス27は、元のままである。

【0030】図9（ニ）は、ネットワーク接続装置9から終端装置6へ送る場合のパケット構成である。送信サブネットワークアドレス22が、ネットワーク接続装置9のサブネットワークDに関するサブネットワークアドレス（9D）と書き換えられ、宛先サブネットワークアドレス21が終端装置6のサブネットワークアドレス（6D）に書き換えられている。送信元装置ネットワークアドレス28、最終宛先装置ネットワークアドレス27は、元のままである。

【0031】このように、パケットは、途中のサブネットワークやネットワーク接続装置で、どの終端装置からのどの終端装置への通信であるか等が解析されるから、機密保護の保証がないサブネットワークやネットワーク接続装置を経由する場合には、データが盗まれる恐れがある。本発明は、このような問題点を解決することを課題とするものである。

【0032】

【課題を解決するための手段】前記課題を解決するため、本発明では、コネクションレス型パケットにより通信を行うネットワークを構成するため複数のサブネットワークを接続する箇所に設けられ、受け取ったパケットの情報を解析して送出経路を選定し新たなパケットを送出するネットワーク接続装置において、機密保護し得ない範囲を送出経路毎に記憶させておく機密保護必要経路記憶部と、暗号化および復号化処理部と、パケットの最終宛先に基づいて選定した転送経路が前記機密保護必要経路記憶部に記憶されている機密保護必要経路を通過するものである場合にパケットのネットワーク層に関するデータの暗号化を決定する暗号化決定部と、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置を前記暗号化したデータの最終宛先として処理するカプセル化部とを具え、カプセル化したデータをパケットに組み込んで送出することとした。

【0033】また、コネクションレス型パケットを用いて通信する複数のサブネットワークがネットワーク接続装置を介して接続されて成るネットワークにおけるネットワーク通信方式において、送信側のネットワーク接続装置では、受け取ったパケットの最終宛先までの経路中に機密保護し得ない範囲が含まれている場合に、受け取ったパケットのネットワーク層に関するデータを暗号化し、前記範囲を越えた箇所にあるネットワーク接続装置を前記暗号化したデータの最終宛先として新たなパケットに組み込んで送出し、最終宛先とされたネットワーク接続装置では、暗号化されたデータを復号化して次へ送出することとした。

【0034】

【作 用】本発明では、コネクションレス型パケットを用いて通信する複数のサブネットワークがネットワーク接続装置を介して接続されて成るネットワークにおいて、機密保護し得ないサブネットワークを挟んだ地点間

で機密の通信をしようとする場合に、それらの地点に、特別の構成を持ったネットワーク接続装置を設置する。

【0035】このネットワーク接続装置では、そこから送信する経路中に機密保護し得ない範囲がある場合には、最初の送信終端装置および最後の宛先終端装置のアドレス情報を含めてデータを暗号化し、それを機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置宛のパケット構成にして送る（カプセル化）。それを受け取ったネットワーク接続装置は、暗号化されたデータを復号化し、最終宛先の終端装置へ、通常のパケット構成で送る。

【0036】機密保護し得ない範囲内にあっては、その範囲を抜けたところに位置するネットワーク接続装置あての通常のパケットという形で通過するから、一体どの終端装置同士の間で通信が行われたのかということを隠すことが出来る。また、データは暗号化されているから、その内容を隠すことが出来る。

【0037】

【実施例】以下、本発明の実施例を図面に基いて詳細に説明する。図1は、本発明のネットワーク接続装置である。符号は図2のものに対応し、40は暗号化・復号化処理部、41はデータカプセル化部、42は暗号化決定部、43は機密保護必要経路記憶部である。これらは、機密保護のために特別に設けられた構成である。このような構成を有するネットワーク接続装置を、機密保護できるサブネットワークと出来ないサブネットワークとの接続部分に設置する。以下、各構成部について説明する。なお、図2と同じ符号のものは同様の動作、機能を果たすので、その説明は省略する。

【0038】機密保護必要経路記憶部43は、どの経路でパケットを送る場合は、どのネットワーク接続装置までは機密保護が保証されていないかを記憶しておく。例えば、図10のネットワーク接続装置7の機密保護必要経路記憶部43は、サブネットワークBの方向に送り出す場合、ネットワーク接続装置9までは機密保護が保証されないと記憶しておく。

【0039】暗号化決定部42は、経路選択部11で選択した経路が機密保護必要経路記憶部43に記憶してある経路に相当するか否かを調べ、相当する場合には、図7のパケットデータ24Dを暗号化することを決定する。暗号化は、暗号化・復号化処理部40で行う。暗号化の手法は、任意のものを採用することが出来る。暗号化・復号化処理部40は、暗号化されたデータを受け取った時に、復号化することも行う。

【0040】データカプセル化部41は、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置をあたかも最終宛先とし、自己のネットワーク接続装置をあたかも最初の送信元として、前記の暗号化データを送信データとしてパケット内に組み込む（これを、説明の便宜上、「カプセル化」ということにする）処理を

する。

【0041】図3は、暗号化データをカプセル化したパケットの構成を示す図である。符号は図7のものに対応し、31はカプセル構成体、32はプロトコルおよびFixedPart、33は最終宛先ネットワーク接続装置ネットワークアドレス、34は送信元ネットワーク接続装置ネットワークアドレス、35はその他の情報部、36は暗号化データ格納部である。

【0042】本発明のネットワーク接続装置で、受け取ったパケットを解析した結果、機密保護が出来ない経路に送り出さなければならないことが判明した時には、ネットワーク層に関するパケットデータ24Dを暗号化し、それを通常のパケットの送信データと同じ扱いとして、暗号化データ格納部36に格納する。

【0043】そして、通常のパケット構成では、最終宛先装置ネットワークアドレス27（図7参照）に相当するところの最終宛先ネットワーク接続装置ネットワークアドレス33に、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置のネットワークアドレスを記載する。また、通常のパケット構成では、送信元装置ネットワークアドレス28（図7参照）に相当するところの送信元ネットワーク接続装置ネットワークアドレス34に、自己のネットワークアドレス即ちパケットを送信しようとしているネットワーク接続装置のネットワークアドレスを記載する。

【0044】図4は、カプセル化データを格納したパケットの具体例を示す。これは、図10のネットワークで、ネットワーク接続装置7、9間は機密保護し得ない範囲であるので、両者間で機密が漏れない通信をするために、ネットワーク接続装置7、9として本発明のネットワーク接続装置を使用しているという環境において、終端装置1から終端装置6へ送るパケットが、ネットワーク接続装置7で作り直された状態のものである。

【0045】符号は図3のものに対応している。送信元装置ネットワークアドレス28のアドレスが終端装置1のネットワークアドレス（1N）とされ、最終宛先装置ネットワークアドレス27が終端装置6のネットワークアドレス（6N）とされたパケットデータ24Dが、そのままの形で暗号化され、暗号化データ格納部36に格納される。送信元ネットワーク接続装置ネットワークアドレス34は、このパケットを今まさに送信しようとしているネットワーク接続装置7のネットワークアドレス（7N）とされている。最終宛先ネットワーク接続装置ネットワークアドレス33は、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置9のネットワークアドレス（9N）とされている。

【0046】送信サブネットワークアドレス22は、このパケットを今まさに送信しようとしているネットワーク接続装置7の、サブネットワークBに関するサブネットワークアドレス（7B）とされ、宛先サブネットワー

クアドレス21は、当面の送り先であるネットワーク接続装置8の、サブネットワークBに関するサブネットワークアドレス(8B)とされている。

【0047】パケットがこのような構成で送られれば、機密保護し得ない途中のネットワーク接続装置では、最初の送信元がネットワーク接続装置7、最終的な宛先がネットワーク接続装置9である通常のパケットとして取り扱われる。従って、真の送信元や真の最終宛先がどこであるかは全く分からないままで、機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置まで送られて行く。また、仮に途中のネットワーク接続装置で送信データを盗もうとしても、その部分は暗号化されているから、内容を知ることが出来ない。

【0048】機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置9も、本発明の構成を有するネットワーク接続装置とされているわけであるが、パケットを受け取ると、暗号化されカプセル化されて来たものかどうか判断する。その判断は、送信元がどこであるかということと(上例の場合、ネットワーク接続装置7)、機密保護必要経路記憶部43に登録されている経路を通して来たかどうかということとを調べて行く。

【0049】暗号化されたものであることが判明した場合には、暗号化・復号化処理部40により元のパケットデータ24Dに復号化し、これを通常のパケット構成で、真の最終宛先である端末装置6へ送る。

【0050】図5は、本発明のネットワーク接続装置の上述したような送信動作を表すフローチャートである。
ステップ1…パケットを受け取る。
ステップ2…受け取ったパケットを解析し、経路を選択し、次に送信する宛先を決定する。
ステップ3…選択した経路が、機密保護の措置をとることが必要な経路かどうかを、機密保護必要経路記憶部43を参照してチェックする。通らなければ、機密保護の措置をとることなく次へ送信する。
ステップ4…機密保護を必要とする経路を通る場合は、送信データを最終宛先および最初の送信元の情報を含めて暗号化する。
ステップ5…暗号化したデータを、カプセル化する。
ステップ6…次の宛先に送信する。

【0051】なお、本発明のネットワーク通信方式を実施するには、ネットワーク全体のネットワーク接続装置を本発明の構成のものに変える必要はなく、単に機密保護をした通信をしようとしている地点にのみ、本発明のネットワーク接続装置を設置すればよいので、安いコストで容易に実施することが出来る。

【0052】

【発明の効果】以上述べた如く、本発明のネットワーク接続装置およびネットワーク通信方式によれば、機密保護し得ないサブネットワークを挟んだ地点間で機密の通信をしようとする場合に、そこから送信する経路中に機密保護し得ない範囲がある場合には、最初の送信端末装置および最後の宛先端末装置を含めてデータを暗号化し、それを機密保護し得ない範囲を抜けたところに位置するネットワーク接続装置宛のパケット構成にして(カプセル化して)送る。

【0053】そのため、機密保護し得ない範囲内にあっては、その範囲を抜けたところに位置するネットワーク接続装置あての通常のパケットという形で通過するから、一体どの端末装置同士の間で通信が行われたのかということを隠すことが出来る。また、データは暗号化されているから、その内容を隠すことが出来る。

【図面の簡単な説明】

【図1】 本発明のネットワーク接続装置

【図2】 従来のネットワーク接続装置

【図3】 カプセル化データを格納したパケットの一般的な構成を示す図

【図4】 カプセル化データを格納したパケットの具体例を示す図

【図5】 本発明のネットワーク接続装置の送信動作を表すフローチャート

【図6】 Black のサブネットワークとWhite のサブネットワークとが含まれているネットワークの1例を示す図

【図7】 パケットの構成を示す図

【図8】 開放型システム間相互接続の基本参照モデルを示す図

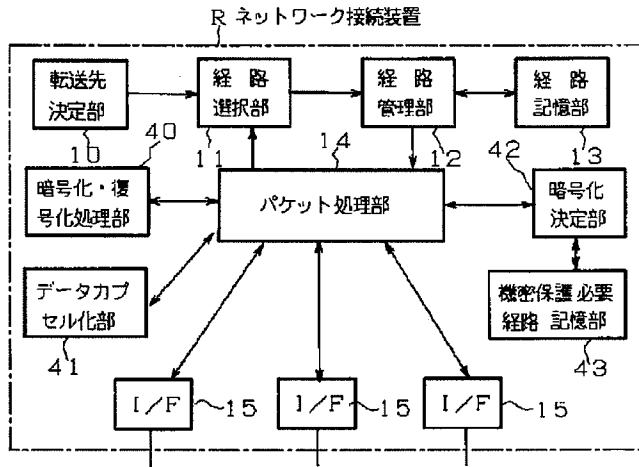
【図9】 図10のネットワークを搬送されるパケットの構成の変化を示す図

【図10】 複数のサブネットワークから成るネットワークの他の例を示す図

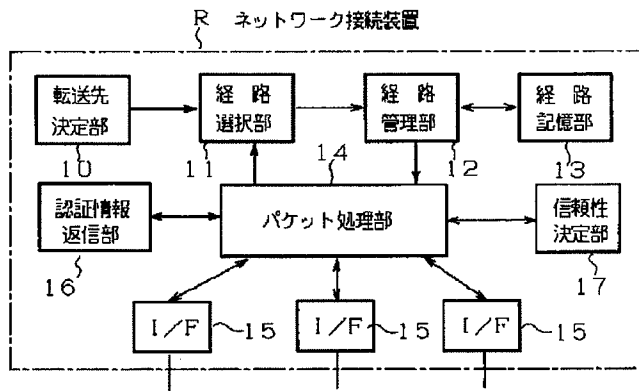
【符号の説明】

1～6…端末装置、7～9…ネットワーク接続装置、10…転送先決定部、11…経路選択部、12…経路管理部、13…経路記憶部、14…パケット管理部、15…インタフェース、16…認証情報返信部、17…信頼性決定部、20…パケット、24D、24D₁、24D₂…パケットデータ、31…カプセル構成体、40…暗号化・復号化処理部、41…データカプセル化部、42…暗号化決定部、43…機密保護必要経路記憶部、50～56…ネットワーク接続装置、57～59…端末装置、A～H、K…サブネットワーク、Rはネットワーク接続装置

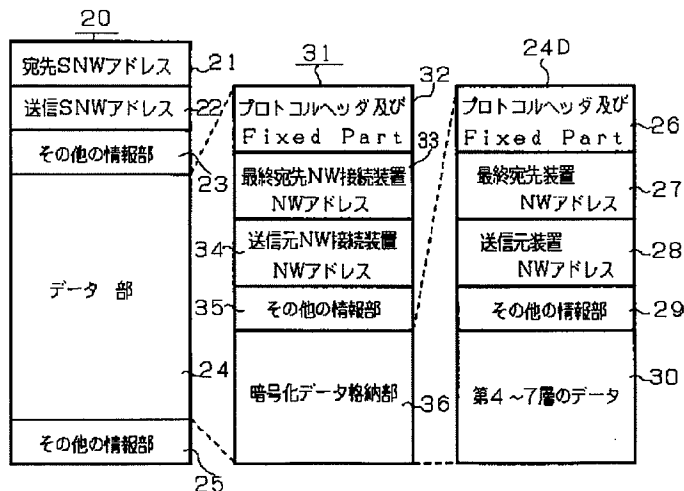
【図1】



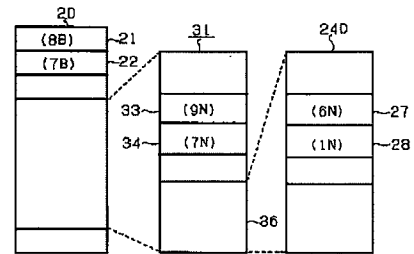
【図2】



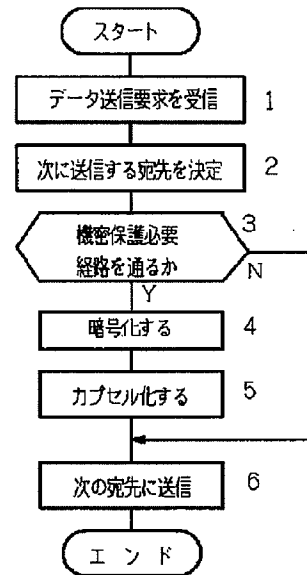
【図3】



【図4】



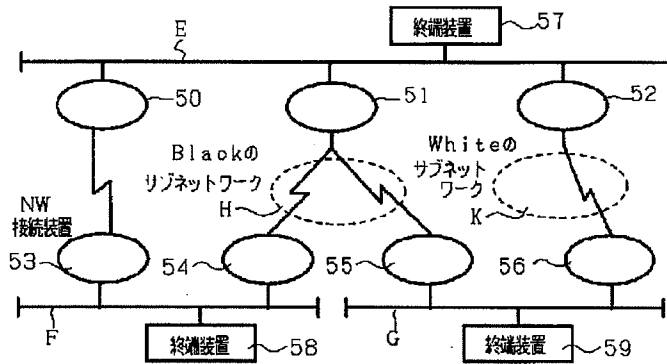
【図5】



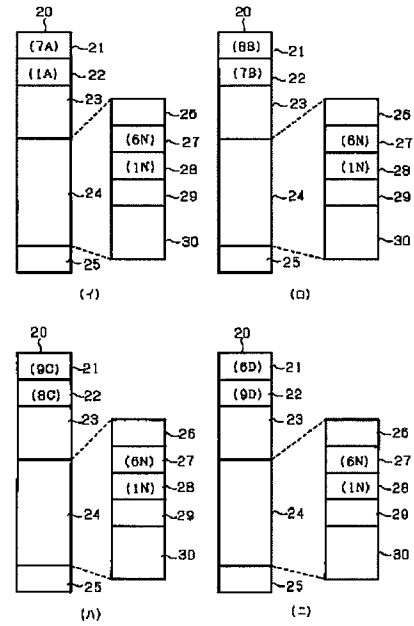
【図8】

局番号	層名称
7	アプリケーション
6	プレゼンテーション
5	セッション
4	トランスポート
3	ネットワーク
2	データリンク
1	物理

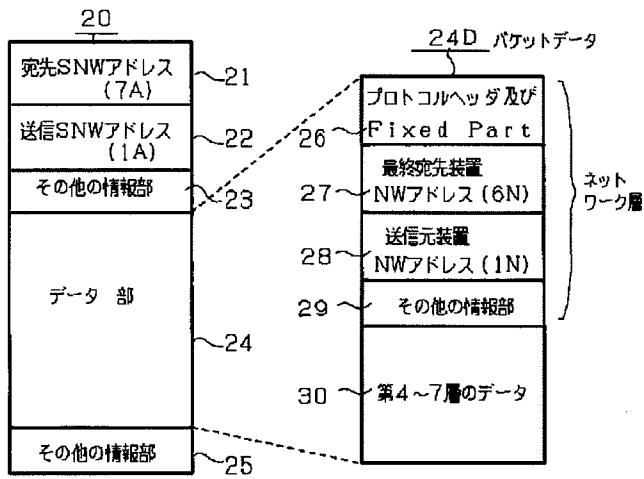
【図6】



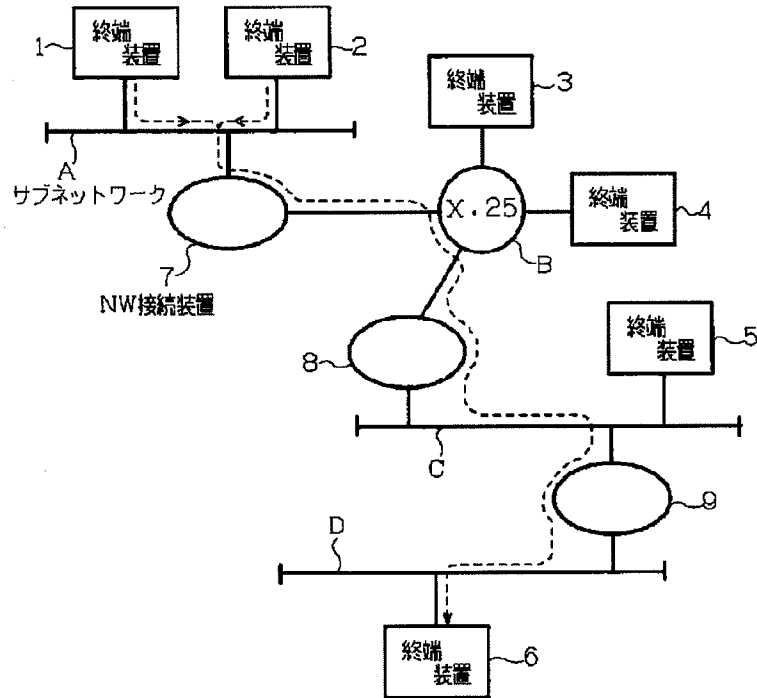
【図9】



【図7】



【図10】



フロントページの続き

(51) Int. Cl. 5

H 0 4 L 9/12

12/28

12/56

識別記号

庁内整理番号

F I

技術表示箇所

8529-5K

H 0 4 L 11/00

3 1 0 C

8529-5K

11/20

1 0 2 D